REMARKS

I. Rejection of claims 1 and 3-23 under 35 USC 112.

Claims 1 and 3-23 are rejected under 35 USC 112 first paragraph as failing to contain subject matter in the specification described in such a way as to reasonably convey to one skilled in the art, that the inventor, at the time the application was filed, had possession of the claimed invention. Specifically, it is stated that independent claims 1, 6, 14, 21 and 23 each recite "said application specific context information supporting acquisition from said second application of information associated with a current operational context of said first application" and there is no mention in the specification of a current operational context of any application, nor of the acquisition of any data.

Contrary to the Rejection statement, not only is the feature concerned recited in the specification in a manner fully compliant with 35 USC 112, it is also explicitly recited in a detailed comprehensive URL processing operational example presented on pages 11-13 and further graphically presented in Figure 2. Specifically, the feature is shown beginning in command step 234 and proceeding through command steps 233, 237 and 239 of Figure 2. A user initiates a query (i.e., an acquisition) in command 234 for laboratory results of a patient ("the URL data and hash value are passed to application 230 via command 234. A user selects the embedded URL link (browser command 207) on browser 10 to view a patient laboratory results, for example"). The query is processed as stated in the Application on page 12 lines 8-24 "in this example application 200 encrypts a patient identifier *(Pid)" (current context information)* for "communication to application 230. The word "current" means "belonging to the present time" (Webster's II New College Dictionary 1995) and in the claim is a descriptive adjective indicating the existing or present operational context of the first application, specifically the current (present or existing) patient identifier of the lab results link of browser command 207, for example, such as selection of link 33 of Figure 1, to initiate command 234. Further, the meaning of current operational context is readily apparent to one of ordinary skill in the art in view of the Application description.

The Application description also indicates "the system protocol employed by manager 250 (and applications 200 and 230) determines that data to be encrypted is collated into an individual MIME (Multipurpose Internet Mail Extension) format data field for encryption into one string. Therefore, as an example,

the string

GSH=24017&Pid=1772693

is encrypted into the string

16sfdjwhejeyw7rh3hekw

Application 200 encrypts the string using a two-key triple DES (Data Encryption Standard) algorithm in cipher block chaining mode employing a 64 bit block and an effective 112 bit key length. The resulting cipher text complies with the URL query data encoding format" (*a query by definition acquires information*) and "represents a single value of a "key = value" pair" (Application). In command steps 233 and 237 "Manager 250 identifies an authenticated user of child application 230 from previously stored identification data eliminating the need for a user to logon again to access child application 230. This constitutes a silent logon process. A child application providing access to other child applications generates URL links (to the other child applications) incorporating the session identifier and additional context information as required" (Application page 8 lines 17-19 and page 14 lines 1-9). Further, "Application 230, in command 239, returns a web page including patient laboratory results" (*the acquired information associated with a current operational context patient identifier of first application 200*) "(previously requested via browser command 207) for display via browser application 10". Therefore, contrary to the Rejection statement on page 6, there is full detailed exemplary support of "said application specific context information supporting acquisition from said second application of information associated with a current operational context of said first application" and exemplary acquisition of data.

The test of enablement under 35 USC 112, as recited in *United States v. Telectronics, Inc.*, 857 F.2d 778, 785, 8 USPQ2d 1217, 1223 (Fed. Cir. 1988) is whether one reasonably skilled in the art could make or use the invention from the disclosures in the patent coupled with information known in the art without undue experimentation". There is ample disclosure of the feature concerned both in the drawings and specification without any need for any "experimentation". Consequently, it is submitted this feature is fully supported and the withdrawal of the Rejection under 35 USC 112 is respectfully requested.

II. Objection to Specification under 35 USC 112.

The specification is objected to as failing to provide proper antecedent basis for the claimed subject matter. Specifically, it is stated that there is insufficient antecedent basis in independent claims 1, 6, 14, 21 and 23 for the limitation "said application specific context information supporting acquisition from said second application of information associated with a current operational context of said first application". Further, that there is no mention in the specification of a current operational context of any application, nor of the acquisition of any information.

Contrary to the Rejection statement, not only is the feature concerned recited in the specification in a manner providing antecedent basis and fully compliant with 35 USC 112, it is also explicitly recited in a detailed comprehensive URL processing operational example presented on pages 11-13 and further graphically presented in Figure 2 as previously explained in connection with the response to the Rejection of claims 1 and 3-23 under 35 USC 112. The example of operation disclosed is more than adequate to enable one of ordinary skill in the art to implement the invention.

III. Rejection under 35 U.S.C. 103(a)

Claims 1 and 3-23 are rejected under 35 U.S.C. 103(a) as being unpatentable over U.S. Patent 6,178,511 – Cohen et al in view of U.S. Patent 5,708,780 – Levergood et al. and further in view of U.S. Patent 5,903,889 – de la Huerga et al. These claims are considered patentable for the following reasons.

Claim 1 recites a system "used by a first application for managing user access to at least one of a plurality of network compatible applications" comprising "an authentication processor for, receiving user identification information including a user identifier and initiating authentication of said user identification information using an authentication service; and at least one communication processor for, communicating an authentication service identifier and a corresponding user identifier to a managing application, said authentication service identifier identifying an authentication service used to authenticate identification information of said corresponding user and automatically communicating application specific context information in a data field of a URL separately from session identification information, to a second application of said plurality of network compatible applications in response to a user command to initiate execution of said second application and in response to authentication of said user identification information, said application specific context information supporting acquisition from said second

application of information associated with a current operational context of said first application". These features are not shown or suggested in Cohen with Levergood and de la Huerga either individually or in combination.

The system of amended claim 1 includes "automatically communicating **application specific context** information in a **data field of a URL** separately from session identification information, to a second application of said plurality of network compatible applications in response to a user command to initiate execution of said second application and in response to authentication of said user identification information". Such application specific context information includes a patient identifier or user identifier, for example (Application page 10 lines 35-37). The claimed system advantageously "automatically" communicates "**application specific context** information in a data field of a URL **separately** from session identification information, to a second application of said plurality of network compatible applications" such as a patient identifier "in response to authentication of said user identification information" initiated by the "authentication processor". Further, the "application specific context information" supports "acquisition" from the "second application of information associated with a current operational context of said first application".

Thereby the system enables a user to logon and authenticate with a first application such as a patient census application and gain automatic access to multiple other applications such as a medical laboratory test result application and in response to user authentication with the test result application, be automatically provided with desired test results for the specific patient selected in the first patient administration application (see example described on Application page 5 lines 8-12 and elsewhere in connection with Figure 2). This is done without the user having to re-enter context information (e.g., a patient identifier) by another command following automatic authentication with a second application. This capability is not shown or suggested in Cohen with Levergood and de la Huerga. The combination of automatic authentication to multiple applications together with automatic communication of application specific context information "in response to a user command to initiate execution of said second application and in response to authentication of said user identification information" facilitates user friendly operation and user seamless navigation in a plurality of concurrently operating applications. The system addresses the problems involved in "facilitating user initiation (e.g., logon), operation and termination (e.g., logoff) of multiple Internet applications and in securely passing URL, patient (and user) identification and other information between applications. A

managing application is employed to coordinate user operation sessions. Specifically the managing application coordinates inactivity timeout operation and maintains and conveys properties between concurrent applications in order to **create a smooth user operation session**" (Application page 4 lines 23-31).

The Rejection on page 8 recognizes that Cohen does not disclose "automatically" communicating "application specific **context** information" in "a data field of a URL" to a "second application of said plurality of network compatible applications" in "response to authentication of said user identification information" initiated by the "authentication processor". However, Levergood (with Cohen) in column 4 lines 1-18 relied on in the Rejection on page 4 also fails to show or suggest "automatically" communicating "application specific **context** information" (such as a patient identifier) in "a data field of a URL" to a "second application of said plurality of network compatible applications" in "response to authentication of said user identification information" initiated by the "authentication processor". Levergood discloses appending session identification information (SID) to a URL (column 3 line 39) and as indicated in the Rejection, the Levergood SID may incorporate a user identifier (Column 5 lines 56-60). However, the Levergood SID is used for authentication and determining access to documents ("a user is provided with a session identification which allows the user to access to the requested file as well as any other files within the present protection domain" - Levergood Abstract).

Consequently, Levergood with Cohen cannot "automatically" communicate "application specific **context** information" (such as a patient identifier) in "a data field of a URL" to a "second application of said plurality of network compatible applications" in "**response to authentication** of said user identification information". Since the context information relied on in the Rejection is within the SID used to authenticate user access to data it cannot be "automatically" communicated in "**response to authentication**". Further, the Levergood SID is not "application specific **context** information" and does NOT support "acquisition from said second application of information associated with a current operational context of said first application" since it is within the SID used for the entirely different purpose of authentication.

As recognized in the Rejection on page 9, Levergood with Cohen fails to show or suggest "automatically" communicating "application specific **context** information" (such as a patient identifier) in "a data field of a URL **separately from session** identification information". However, contrary to the Rejection statement on

page 9, de la Huerga (with or without Levergood and Cohen) also does not show or suggest "automatically" communicating "application specific **context** information" in "a data field of a URL **separately from session** identification information". De la Huerga in column 10 lines 43-59 and Figure 14A shows a URL conveying "application specific **context** information" (a patient identifier) in "a data field of a URL" but does NOT show or suggest a URL conveying "**session** identification information" in a separate data field of the URL. The items relied on in the Rejection in de la Huerga column 10 lines 43-59 have nothing to do with a computer "session" and de la Huerga nowhere even mentions or contemplates "session". De la Huerga column 10 lines 43-59 states "Embedded in this URL address 700 is information regarding the type of data 704, the patient's identification 708, the date 712 and time 716 of the data requested, and a report designator 718". The "date 712 and time 716 of the data requested" are the time and date associated with a report accessed via the URL and have nothing to do with a computer "session". Similarly, "report designator 718" is a designator, e.g., name or other identifier of the report accessed. The Rejection allegation on page 9 that items 712, 716 and 718 have anything to do with a computer "session" is erroneous, unfounded speculation. These items provide no 35 USC 112 compliant enabling disclosure of "automatically" communicating "application specific **context** information" in "a data field of a URL **separately from session** identification information".

A "session identifier" identifies a session of computer operation including one or more executable applications (a "session identifier is used by applications 200 and 230 to identify a user initiated session in communicating with manager 250" – Application page 5 lines 29-32, "Specifically the managing application coordinates inactivity timeout operation and maintains and conveys properties between concurrent applications in order to create a smooth user operation session. " Application page 4 lines 27-30). This is corroborated in Levergood (a "user is provided with a session identification which allows the user to access to the requested file as well as any other files within the present protection domain" - Levergood Abstract). Therefore, "session identification information" is NOT (and is not suggested by) a "date 712 and time 716" of associated with requested report data accessed via a URL or a "report designator 718" e.g., name or other identifier of the report accessed. Further, session identification information is not "application specific **context** information" and does NOT support "acquisition from said second application of information associated with a current operational context of said first application". Though Levergood discloses appending session identification information (SID) to a URL (column 3 line 39), session identification is used for

authentication and determining access to documents (a user is provided with a session identification which allows the user to access to the requested file as well as any other files within the present protection domain" - Levergood Abstract). Session identification information is not "application specific **context** information" and does NOT support "acquisition from said second application of information associated with a current operational context of said first application". Cohen with Levergood and de la Huerga also does not suggest the automatic feature combination comprising "automatically" communicating "application specific context information" in "a data field of a URL separately from session identification information" together with facilitating automatic authentication to multiple network compatible applications" by "communicating an authentication service identifier" and a "corresponding user identifier to a **managing application**". This provides seamless navigation advantages not shown or suggested in the combined references.

Further, incorporating the de la Huerga features in Cohen with Levergood as suggested in the Rejection results in the system burden of requiring a user to initiate at least a second command (e.g., a URL link selection) conveying application specific context information to an Application **in addition to** initiating a first command conveying session identification information (e.g., a URL link selection) to the Application. The claimed arrangement in contrast uses a single command to seamlessly achieve this navigation. Further the absence of any common problem recognition, advantage identification or other motivation in the three references undermines any suggestion that combining these disparate systems would be obvious to one of ordinary skill in the art. Further, the Rejection fails to provide any showing of how such disparate systems may be combined when each system has features that conflict with systems employed by the other references (in security management, URL format, handshaking etc.). Consequently withdrawal of the Rejection of amended claim 1 under 35 USC 103(a) is respectfully requested.

Dependent claim 3 is considered to be patentable based on its dependence on claim 1. Claim 3 is also considered to be patentable because Cohen with Levergood and de la Huerga does not show or suggest a system in which "a communication processor of said at least one communication processor also communicates a session identifier identifying a user initiated session of operation of said first application to said managing application and said user identification information includes a password associated with said user identifier". As previously explained in connection with claim 1, Cohen with Levergood and de la Huerga does not suggest "automatically" communicating "application specific **context**

information" comprising "a **patient** identifier" in "a data field of a URL **separately from session identification** information".

Dependent claim 4 is considered to be patentable based on its dependence on claim 1. Claim 4 is also considered to be patentable because Cohen with Levergood and de la Huerga does not show or suggest a system in which "a communication processor of said at least one communication processor communicates said authentication service identifier and said corresponding user identifier to a managing application for compilation of a database". Contrary to the Rejection statement on page 5, Cohen in Column 4 line 61 to column 5 line 6, lines 16-22 and 45-58 does not suggest "**compilation** of a database" including "**authentication service identifier** and said corresponding user identifier" data pairs. Cohen with Levergood and de la Huerga column 4 line 61 to column 5 line 6 recites "Preferably, PKM 24 is a secure, globally accessible repository that facilitates the single sign-on process. Although not meant to be limiting, with respect to a given user, the PKM (as will be described) preferably stores such information as a *username, a set of one or more password(s), and any other application environment-specific information such as domain name, hostname, application name, and the like.* Because this access information preferably is centralized in the PKM, users can access their target resources with one sign-on from any workstation. They can also manage their passwords from this one repository, as will also be seen". It is well understood that citation of a **general** list of items such as those italicized fail to provide 35 USC 112 compliant enabling disclosure of **specific** elements such as the recited "authentication service identifier and said corresponding user identifier" data pairs. Further, Cohen with Levergood and de la Huerga fails to show or suggest **communicating** "said authentication service identifier and said corresponding user identifier **to** a **managing application** for **compilation** of a database". In Cohen with Levergood and de la Huerga there is no suggestion of dynamic "**compilation**" of a database. There is no indication in Cohen with Levergood and de la Huerga of HOW the PKM repository is provided or any indication other than it is predefined and NOT provided by dynamic "compilation".

Dependent claim 5 is considered to be patentable based on its dependence on claims 1 and 4. Claim 5 is also considered to be patentable because Cohen with Levergood and de la Huerga does not show or suggest a feature combination as in claim 5 involving a database "accessible by other applications of said plurality of network compatible applications for mapping a non-authenticated

user identifier of a participant application to an authenticated and different user identifier of another application".

Independent claim 6 recites a "system used for processing user access to network compatible applications" comprising "an authentication processor for, receiving authentication service identifier and corresponding user identifier data pairs from at least one of a plurality of applications, compiling a database using said data pairs, mapping a non-authenticated user identifier of a second application to an authenticated different user identifier of a first application using said database; and at least one communication processor for, communicating said authenticated different user identifier to said second application and automatically communicating application specific context information in a data field of a URL separately from session identification information, to said second application in response to a user command to initiate execution of said second application, said application specific context information supporting acquisition from said second application of information associated with a current operational context of said first application".

Amended independent claim 6 is considered to be patentable for the reasons given in connection with claims 1, 4 and 5. Claim 6 is also considered to be patentable because Cohen with Levergood and de la Huerga does not show (or suggest) a feature combination as in claim 6 including "compiling a database" using "data pairs, mapping a non-authenticated user identifier of a second application to an authenticated different user identifier of a first application using said database" and at least one communication processor for, "automatically communicating application specific context information in a data field of a URL **separately from session** identification information, to said second application in response to a user command to initiate execution of said second application". Cohen with Levergood and de la Huerga does not show or suggest "compilation of such a database" in combination with automatically communicating application specific context information in a data field of a URL **separately** from session identification information, to said second application in response to a user command to initiate execution of said second application". Cohen with Levergood and de la Huerga also does not mention, contemplate or suggest "automatically communicating" "application specific context information supporting acquisition from said second application of information associated with a **current** operational context of said **first application**".

As recognized in the Rejection, Levergood with Cohen fails to show or suggest "automatically" communicating "application specific **context** information"

(such as a patient identifier) in "a data field of a URL **separately from session** identification information". However, contrary to the Rejection statement on page 9, de la Huerga (with or without Levergood and Cohen) also does not show or suggest "automatically" communicating "application specific **context** information" in "a data field of a URL **separately from session** identification information". De la Huerga in column 10 lines 43-59 and Figure 14A shows a URL conveying "application specific **context** information" (a patient identifier) in "a data field of a URL" but does NOT show or suggest a URL conveying "**session** identification information" in a separate data field of the URL. The items relied on in the Rejection in de la Huerga column 10 lines 43-59 have nothing to do with a computer "session" and de la Huerga nowhere even mentions or contemplates "session". De la Huerga column 10 lines 43-59 states "Embedded in this URL address 700 is information regarding the type of data 704, the patient's identification 708, the date 712 and time 716 of the data requested, and a report designator 718". The "date 712 and time 716 of the data requested" are the time and date associated with a report accessed via the URL and having to do with a computer "session". Similarly, "report designator 718" is a designator, e.g., name or other identifier of the report accessed. The Rejection allegation on page 9 that items 712, 716 and 718 have anything to do with a computer "session" is erroneous, unfounded speculation. These items provide no 35 USC 112 compliant enabling disclosure of "automatically" communicating "application specific **context** information" in "a data field of a URL **separately from session** identification information".

A "session identifier" identifies a session of computer operation including one or more executable applications (a "session identifier is used by applications 200 and 230 to identify a user initiated session in communicating with manager 250" – Application page 5 lines 29-32, "Specifically the managing application coordinates inactivity timeout operation and maintains and conveys properties between concurrent applications in order to create a smooth user operation session. " Application page 4 lines 27-30). This is corroborated in Levergood (a "user is provided with a session identification which allows the user to access to the requested file as well as any other files within the present protection domain" - Levergood Abstract). Therefore, "session identification information" is NOT (and is not suggested by) a "date 712 and time 716" of associated with requested report data accessed via a URL or a "report designator 718" e.g., name or other identifier of the report accessed. Further, session identification information is not "application specific **context** information" and does NOT support "acquisition from said second application of information associated with a current operational context of said first

application". Though Levergood discloses appending session identification information (SID) to a URL (column 3 line 39), session identification is used for authentication and determining access to documents (a user is provided with a session identification which allows the user to access to the requested file as well as any other files within the present protection domain" - Levergood Abstract). Session identification information is not "application specific **context** information" and does NOT support "acquisition from said second application of information associated with a current operational context of said first application". Cohen with Levergood and de la Huerga also does not suggest the automatic feature combination comprising "automatically" communicating "application specific context information" in "a data field of a URL separately from session identification information" together with facilitating automatic authentication to multiple network compatible applications" by "communicating an authentication service identifier" and a "corresponding user identifier to a **managing application**". This provides seamless navigation advantages not shown or suggested in the combined references.

Further, incorporating the de la Huerga features in Cohen with Levergood as suggested in the Rejection results in a system requiring a user to initiate at least a second command (e.g., a URL link selection) conveying application specific context information to an Application **in addition to** initiating a first command conveying session identification information (e.g., a URL link selection) to the Application. The claimed arrangement in contrast uses a single command to seamlessly achieve this navigation. Further the absence of any common problem recognition, advantage identification or other motivation in the three references undermines any suggestion that combining these disparate systems would be obvious to one of ordinary skill in the art. Further, the Rejection fails to provide any showing of how such disparate systems may be combined when each system has features that conflict with systems employed by the other references (in security management, URL format, handshaking etc.).

Dependent claim 7 is considered to be patentable based on its dependence on claim 6. Claim 7 is also considered to be patentable because Cohen with Levergood and de la Huerga does not show or suggest the feature combination of claim 7 in which "said authentication service identifier identifies an authentication service used to authenticate identification information comprising a user identifier of said corresponding user to provide an authenticated user identifier". Cohen's mention of "information on how to logon to the applications configured on a given machine" in column 4 lines 48-50 fails to provide 35 USC 112 compliant enabling disclosure of

an "authentication service identifier" that "identifies an authentication service used to authenticate identification information comprising a user identifier of said corresponding user to provide an authenticated user identifier" in combination with the other features of this claim.

Dependent claim 8 is considered to be patentable based on its dependence on claim 6. Claim 8 is also considered to be patentable because Cohen with Levergood and de la Huerga does not show or suggest the feature combination of claim 8 in which "said authentication processor performs said mapping using said database by matching an authentication service identifier of said second application with an authentication service identifier of said first application and providing said authenticated different user identifier of said first application as a mapped user identifier". Cohen column 6 lines 26-37 relied on in the Rejection on page 6 fails to provide 35 USC 112 compliant enabling disclosure of an "authentication processor" that "performs said **mapping** using said database by matching an authentication service identifier of said second application with an authentication service identifier of said first application and providing said **authenticated different user identifier** of said first application as a **mapped user identifier**". These features are not specifically shown or suggested in Cohen with Levergood and de la Huerga.

Dependent claim 9 is considered to be patentable based on its dependence on claim 6. Claim 9 is also considered to be patentable because of reasons given in connection with claim 2.

Dependent claim 10 is considered to be patentable based on its dependence on claim 6.

Dependent claim 11 is considered to be patentable based on its dependence on claim 6. Claim 11 is also considered to be patentable because Cohen with Levergood and de la Huerga does not show or suggest the feature combination of claim 11 in which "a communication processor of said at least one communication processor communicates a parameter to said second application, said parameter identifying success or failure of said mapping". The Rejection alleges this feature is shown in Cohen and relies for support on column 10 lines 35-37 ("Return codes from the interface are associated with buckets (rc_ success, rc_error, etc.), allowing the appropriate action to be taken based on the bucket into which the return code falls"). However, "Return codes... allowing the appropriate action to be taken based on the bucket into which the return code falls" does not show or suggest (or provide a 35

USC 112 enabling disclosure of) communicating "a parameter to said second application...identifying success or failure of" "mapping a non-authenticated user identifier of a second application to an authenticated different user identifier of a first application using" a compiled "database". The Return codes in Cohen appear to be related to logon success (column 10 lines 22-29) and have nothing to do with success of "mapping a non-authenticated user identifier of a second application to an authenticated different user identifier of a first application using said database" in "compiling a database". As previously explained Cohen with Levergood and de la Huerga does not discuss dynamic "compilation" of such a database at all.

Dependent claims 12 and 13 are considered to be patentable based on their dependence on claim 6.

Independent claim 14 recites a "system used for processing user access to Internet compatible applications," comprising "an authentication processor for, receiving an authentication service identifier and corresponding user identifier from a parent application, and mapping a non-authenticated user identifier of a child application to an authenticated different user identifier of said parent application; and at least one communication processor for, communicating said authenticated different user identifier to said child application and automatically communicating application specific context information in a data field of a URL separately from session identification information, to said child application in response to a user command to initiate execution of said child application and in response to communicating said authenticated different user identifier, said application specific context information supporting acquisition from said child application of information associated with a current operational context of said parent application". Amended independent claim 14 is considered to be patentable for the reasons given in connection with claims 1, 4, 5 and 6.

Dependent claim 15 is considered to be patentable based on its dependence on claim 14.

Dependent claims 16-20 are considered to be patentable based on their dependence on claim 14 and any intervening claim and because of the additional feature combinations they represent for the reasons given in connection with previous claims.

Independent method claim 21 mirrors apparatus claim 14 and is considered to be patentable for similar reasons.

Dependent claim 22 is considered to be patentable based on its dependence on claim 21 for reasons given in connection with claim 6.

Independent method claim 23 mirrors apparatus claim 1 and is considered to be patentable for similar reasons. Consequently withdrawal of the Rejection of claims 1 and 3-23 under 35 USC 103(a) is respectfully requested.

IV. Rejection under 35 U.S.C. 103(a)

Claim 2 is rejected under 35 U.S.C. 103(a) as being unpatentable over U.S. Patent 6,178,511 – Cohen et al in view of U.S. Patent 5,708,780 – Levergood et al. These claims are considered patentable for the following reasons.

Amended independent claim 2 recites a system "used by a first application for managing user access to at least one of a plurality of network compatible applications" comprising "an authentication processor for, receiving user identification information including a user identifier and initiating authentication of said user identification information using an authentication service; and at least one communication processor for, communicating an authentication service identifier and a corresponding user identifier to a managing application, said authentication service identifier identifying an authentication service used to authenticate identification information of said corresponding user and automatically communicating application specific context information in a data field of a URL to a second application of said plurality of network compatible applications in response to a user command to initiate execution of said second application and in response to authentication of said user identification information wherein said application specific context information comprises at least one of, (a) a user identifier and (b) a patient identifier and a communication processor of said at least one communication processor encrypts an address portion of said URL and incorporates said encrypted address portion of said URL, together with said address portion of said URL in non-encrypted form, into a single processed URL data string". These features are not shown or suggested in Cohen with Levergood and de la Huerga.

Amended independent claim 2 is considered to be patentable for reasons given in connection with claim 1 and for the following reasons. Cohen with

Levergood does NOT discuss or suggest "automatically" communicating "application specific **context** information in a data field of a URL" such as a patient identifier" to a "second application of said plurality of network compatible applications" in "response to authentication of said user identification information" in combination with facilitating automatic authentication to multiple network compatible applications" by "communicating an authentication service identifier" and a "corresponding user identifier to a **managing application**". Cohen with Levergood also fails to show or suggest encrypting an "**address portion** of said URL link" to the "second application" and incorporating the "encrypted address portion of said URL, together with said address portion of said URL in non-encrypted form, into a single processed URL data string". In an exemplary embodiment of the invention illustrated in the Application specification pages 11-12, application 200 advantageously, for example, encrypts "a **URL** link **address portion**" comprising a hash value identified by field identifier GSH= derived by "hashing on the **addressable portion** of a fully qualified URL" comprising the "URL data either lying between the "http://" and the question mark "?" or from the data lying between the "http://" and the pound/number sign "#" - whichever comes first" (Application page 9 lines 31-33 and page 11 line 25). Consequently, in the exemplary URL string shown processed in the specification page 12

> www.smed.com/altoona/prd/results.exe/1?GSM=16253384937&GSH=24017&Pid=1772693&Frgclr=blue

the compressed address portion is 24017 which is concatenated with a patient identifier (Application page 12 line lines 15-20) as shown:

> GSH=24017&Pid=1772693

and is encrypted into the string

> 16sfdjwhejeyw7rh3hekw

to produce the processed URL including the encrypted URL address portion:

> www.smed.com/altoona/prd/results.exe/1?GSM=16253384937:16sfdjwhejeyw7rh3hekw&Frgclr=blue.

This is an exemplary "processed URL". The Rejection makes a **fundamental error**

on page 5 in interpreting the Levergood reference. Contrary to the Rejection statements on page 5, Levergood in column 4 line 64 to column 5 line 2, column 5 lines 56-65 and column 3 lines 34-37 relied on in the Rejection merely discloses encryption of a session identifier (SID) and an IP address. Specifically, Levergood states "the digital signature is a cryptographic hash of the remaining items in the SID and the authorized IP address which are encrypted with a secret key which is shared by the authentication and content servers"- Levergood column 5 lines 61-65, also see column 3 lines 33-37).

Further, although in Levergood a valid session identifier "typically comprises" an "accessible domain" in the "SID encrypted with a secret key", the Levergood accessible domain is NOT a URL or an address portion of a URL (Levergood column 3 lines 33-37). Levergood explicitly defines an accessible "domain" as a collection of files and NOT a URL or address portion of a URL ("A protection domain is **defined** by the service provider and is a **collection of controlled** files of common protection within one or more servers" – Levergood column 3 lines 52-55). This is further made clear in column 5 lines 54-61 stating a "preferred SID is a sixteen character ASCII string that encodes **96** bits of SID data" that contains "an 8-bit **domain** comprising **a set of information files** to which the current SID authorizes access". Such an "accessible domain" as used by Levergood is not in a URL link address portion. This is further corroborated in Levergood in column 6 lines 29-34 indicating that such a domain is in the non-address, URL data field portion of a URL (e.g. after the question mark), specifically, a "REDIRECT URL might be: "http://auth.com/authenticate?**domain**= [domain]& URL = http://content.com/report".

Levergood does not show or suggest encrypting an "**address portion** of said URL link" to the "second application" and incorporating the "encrypted address portion of said URL, together with said address portion of said URL in non-encrypted form, into a single processed URL data string". Neither a session identifier nor an IP address as used in Levergood are a "URL or a URL address portion". Indeed a URL and IP address are distinct and different objects with totally different functions ("the content server records the URL **and** the IP address" – Levergood column 5 lines 37-38). An IP address describes an electronic address of an Internet entity whereas a URL "consists of three parts: the transfer format, the host name of the machine that holds the file, and the **path** to the file" (Levergood column 2 lines 28-31). A session identifier identifies a user session of computer operation for example and is itself a distinct entity that may be conveyed within a field of a URL (Application page 11 line 17).

The Rejection states in the response to Arguments section on page 3 that if the domain includes a collection of files within a server, then the "domain must include an identification and/or address for these files", thus the domain can indeed include an address portion of a URL. However, nowhere in Levergood et al. is it disclosed or suggested that the domain includes a URL or even a portion of a URL. In fact, Levergood et al. explicitly defines a protection domain as "a collection of controlled files of common protection within one or more servers" in column 3, lines 52-55. The Examiner's reliance on interpreting "a collection of files" to anticipate "using a received encryption key to encrypt a URL link address portion" is a **fundamental error.** In so doing, the Examiner is not only engaging in the pure speculation that the Levergood "collection of files" has something to do with a URL, but also that it leads to teaching encryption of a "URL address portion" as specifically defined in the present Application. Further, this speculation is without foundation and **directly contradicts** Levergood's own teaching in column 5 line 59 that a domain is an 8 – bit value ("SID data" contains "an 8-bit **domain** comprising **a set of information files**"). Thus, Levergood et al. neither disclose nor suggest "a URL processor for adaptively processing a URL link" as in the present claimed invention.

The purpose of the Levergood encryption is to ensure validity of session identifiers (SIDs) by using an "Internet server" to subject "the client to an authorization routine prior to issuing the SID" (Levergood column 3 lines 24-26). In contrast, the Application addresses the problem of preventing "URL replay or redirection" through its recognition that URLs are "vulnerable to corruption" (Application page 11 lines 1-9). Consequently there is no reason, problem recognition or motivation for amending the Levergood system to include the claimed arrangement. Consequently, withdrawal of the rejection of claim 2 under 35 USC 103(a) is respectfully requested.

In view of the above amendments and remarks, Applicants submit that the Application is in condition for allowance, and favorable reconsideration is requested.

Respectfully submitted,

Date: November 1, 2005

Alexander J. Burke
Reg. No. 40,425

Siemens Corporation,
Customer No. 28524
Tel. 732 321 3023
Fax 732 321 3030